USER IDENTITY PROTECTION IN A WIRELESS LAN-UNIVERSAL MOBILE TELEPHONE SYSTEM INTERWORKING ARRANGEMENT

CROSS REFERENCE TO RELATED APPLICATION

This application claims priority under 35 U.S.C. 119(e) to U.S. Provisional Patent Application Serial No 60/403,159, filed August 13, 2002, the teachings of which are incorporated herein.

TECHNICAL FIELD

This invention relates to a technique for protecting the identity of the user of a mobile wireless terminal upon a transition from one wireless network to another.

BACKGROUND ART

Advances in the field of wireless LAN technology has led to the availability of relatively inexpensive wireless LAN equipment, which, in turn, has resulted in the emergence of publicly accessible wireless LANs (e.g., "hot spots") at rest stops, cafes, libraries and similar public facilities. Presently, wireless LANs offer users access to a private data network, such as a Corporate Intranet, or a public data network such as the Internet. Few if any publicly accessible wireless LAN's offer any type of telephone service, let alone, wireless telephony service.

Presently, users seeking wireless telephony service typically subscribe to one of many providers of such service. Today's wireless telephony service providers not only offer voice calling but also offer General Packet Radio Service (GPRS) to enable the exchange data packets via a mobile wireless terminal. While GPRS exists in many areas, data transmission rates typically do not exceed 56 Kbps and the costs to wireless network service providers to support this service remain high, making GPRS expensive.

To provide enhanced data communications, efforts are underway to establish new standards for wireless telephony. One such effort is the proposed "Universal Mobile

Telecommunications System (UMTS) " standard specified by the 3rd Generation Partnership Project (3GPP) for advanced packet radio service in wireless telephony networks. The UMTS standard proposes transmission rates as high as 2 Mbps. However, the relatively low cost to implement and operate a wireless LAN, as well as the available high bandwidth (usually in excess of 10 Megabits/second) makes the wireless LAN a preferred access mechanism, even as compared to a UMTS network. Given the advantage of lower cost and higher bandwidth, mobile wireless terminal users will often seek to transition to a wireless LAN when such service is available. When wireless LAN service becomes no longer available, the user will transition back to the wireless telephony network.

Access to the wireless telephony network and the wireless LAN both require user identification and verification. From the perspective of the network operator, revenue generation depends on reliable user identification and verification. Absent correct user identification and validation, the network operator will likely be unable to bill for such services. From the user's perspective, identification and verification should occur in a manner that safeguards against identity fraud. Thus, user identification should not occur in a manner that would allow others to make improper use of such information.

Presently, a user seeking access to a wireless telephony network receives a temporary identity, known as a Packet Temporary Mobile Subscriber Identity (P-TMSI). Typically, a Visited Location Register (VLR) attached to Serving GPRS Support Node (SGSN) in the wireless telephony network maintains a copy of the user's P-TMSI. The SGSN maps the P-TMSI to a permanent identity, known as the International Mobile Subscriber Identity (IMSI). To avoid compromising the user's identity, the wireless telephony network will assign the user a different P-TMSI if a long interval has elapsed since a previous identification.

Current wireless LANs lack secure user identification and verification mechanisms. A potential security risk currently exists for users seeking to transition to a wireless LAN from a wireless telephony network.

Thus, there is a need for a technique for protecting the identity of a user when transitioning from one wireless network to another.

BRIEF SUMMARY OF THE INVENTION

Briefly, in accordance with a preferred embodiment of the present principles, there is provided a method for identifying the user of a mobile wireless terminal upon transitioning from a first wireless network to a second wireless network. The method commences upon receipt in the second network of a request for identification from the user upon a transition to that network. The identification request includes a temporary identifier previously supplied by the mobile wireless terminal to identify itself in the first wireless network. From the identification request, an identification is made of a node in the first network last accessed by the mobile wireless terminal. Upon identifying the last-accessed node, the identification request received in the second network is forwarded to the last-accessed node in the first network, which in turn, verifies the user's permanent identity from the temporary identifier. Such verification information is then returned to the second network, which in response, grants access to the user upon successful user verification. By sending a temporary identity to identify itself in the second network, the user avoids the need to send its permanent identity during the network transition, which could be intercepted resulting in a breach of security.

BRIEF DESCRIPTION OF THE DRAWING

FIGURE 1 illustrates a block schematic diagram of a wireless telephony network interworked with a wireless LAN for providing communication service to a mobile wireless terminal.

DETAILED DESCRIPTION

FIGURE 1 depicts an illustrative embodiment of a wireless telephony network 12 interworked with a wireless Local Area Network (LAN) 14 to provide communications service to a mobile wireless terminal 16 in accordance with the present principles. In practice, the mobile wireless terminal 16 will attach itself to the wireless telephony network 12 to obtain voice and/or data services. However, for higher speed, lower cost

data access, the user of mobile wireless terminal 16 often will transition from the wireless telephony network 12 to the wireless LAN 14 upon entering the coverage area of the later. A reverse transition occurs when the user leaves the wireless LAN for the wireless telephony network.

In the illustrated embodiment, the wireless telephony network 12 has the architecture proposed in the "Universal Mobile Telecommunications System (UMTS) " standard for advanced packet radio service. Accordingly, the wireless telephony network 12 includes at least one Serving GPRS Support Node (SGSN) 18 for authenticating the mobile wireless terminal 16. The SGSN 18 also serves to process packet data for exchange with the mobile wireless terminal 16 while the terminal communicates with the wireless telephony network 12 through a wireless telephony radio network 20. Although FIG. 1 depicts one wireless telephony radio network 20, the wireless telephony network 12 could include multiple radio networks, each managed by a separate SGSN. A Home Location Register (HLR) 22 in the wireless telephony network 12 stores records of current wireless telephony service subscribers and contains packet domain subscription information as well as location information of which SGSN 18 serves a particular mobile wireless should the wireless telephony network contains more than one SGSN.

The wireless telephony network 12 also includes a wireless LAN (WLAN) interworking access server 24 for managing the interface between the wireless LAN 14 and the wireless telephony network. The WLAN interworking access server 24 performs a function similar to the SGSN 18. Thus, the WLAN interworking server 24 authenticates the mobile wireless terminal. It may or may not process the packet data depending on whether the data connection needs to go through the wireless telephony network or not. In accordance with the present principles, the WLAN interworking access server 24 cooperates with the SGSN 18 to perform secure identification of the mobile wireless terminal 16 upon a transition from the wireless telephony network 12 to the wireless LAN 14 using the P-TMSI provided by the wireless mobile terminal. As described in greater detail below, such identification provides security by obviating the need for the mobile wireless terminal 16 to send a permanent identity.

Upon the very first direct access of the wireless telephony network 12, the mobile wireless terminal 16 will receive a temporary identity, usually referred to as a Packet Temporary Mobile Subscriber Identity (P-TMSI) as part of the registration process.

Upon each subsequent direct access of the wireless telephony network 12, the terminal will deliver its P-TMSI to the corresponding SGSN 18 through the wireless radio network 20. Using its Visited Location Register (VLR) 23, the SGSN 18 maps the P-TMSI to the user's permanent identity, referred to as an International Mobile Subscriber Identity (IMSI) to verify the user of the terminal.

When accessing the wireless telephony network 12, the mobile wireless terminal 16 uses its temporary identity (P-TMSI) such that its real identity need not cross the radio interface after initial registration. In the case of a handoff from one SGSN to another, the new SGSN receives the P-TMSI from the mobile wireless terminal 16. If the new SGSN does not currently serve the mobile wireless terminal user 16, the new SGSN will query the "old" SGSN. By doing so, the new SGSN will retrieve the address of the "old" SGSN that had previously served the mobile wireless terminal 16 and had last mapped the temporary identity of the terminal to its permanent identity. The new SGSN will request that the old SGSN send back the IMSI associated with the temporary address (P-TMSI) previously supplied by the mobile wireless terminal 16.

Heretofore, there did not exist a secure access arrangement that allowed the mobile wireless terminal 16 to transition from the wireless telephony network 12 to the wireless LAN 14 while maintaining the terminal's identity secure from possible interception. Typically, the user of the mobile wireless terminal 16, upon transitioning to the wireless LAN 14, needed to send its permanent identity (i.e., its IMSI) to the wireless LAN 14, thus compromising its identity.

In accordance with the present principles, there is provided a technique for protecting the IMSI of the mobile wireless terminal 16 upon transitioning from one wireless network (the wireless telephony network 12) to the wireless LAN 14. To protect the identity of the user, the technique of the present principles makes use of the user identity information (i.e., the P-TMSI) maintained by the last-attached SGSN (e.g., SGSN 18 of FIG. 1) to verify the user's permanent identity in the wireless LAN 14. Such user identification and verification occurs as follows:

1. Upon transitioning to the wireless LAN 14, the mobile wireless terminal 16 sends the same identity information it previously sent to the wireless telephony network 12. Such identity information includes the old (i.e., previously sent) P-TMSI, P-

TMSI signature and Routing Area Identifier (RAI). As described, the P-TMSI constitutes a temporary user identification. The P-TMSI signature provides verification of the P-TMSI, whereas the RAI distinguishes each SGSN 18 accessible to the mobile wireless terminal 16. Each SGSN 18, as well as the WLAN interworking access server 24, has its own unique RAI. Heretofore, the RAI only identified SGSNs in the wireless telephony network 12. In accordance with an aspect of the present principles, the WLAN interworking access server 24 has its own RAI, so the server appears simply as another SGSN. In this way, the WLAN interworking access server 24 can query an old SGSN with a P-TMSI received from the mobile wireless terminal 16 for the purpose of obtaining the IMSI of the terminal.

2. Upon receipt of the identity information (i.e., the P-TMSI, P-TMSI signature, and RAI), the wireless LAN 14 forwards such information to the WLAN interworking access server 24 in the wireless telephony network 12. From such identity information, the WLAN interworking access server 24 first determines the identity of the old SGSN 18 previously accessed by the mobile wireless terminal 16 immediately prior to transitioning to the wireless LAN 14. Typically, the WLAN interworking access server 24 identifies the old SGSN by finding its address through an association with the old Routing Area in the RAI supplied by the mobile wireless terminal 16. Typically, the WLAN interworking access server 24 knows the address of each SGSN in the wireless telephony network 12 via the HLR 22. In the event that the WLAN interworking access server 24 does not know the address of the old SGSN 18, the server can acquires the address from a Domain Naming System (DNS) server (not shown) using a logical address provided by the mobile wireless terminal 16.

3. After identifying the old SGSN 18, the WLAN interworking access server 24 then sends the P-TMSI, P-TMSI signature and RAI to the old SGSN 18 to request the user's IMSI.

4. In response to the request from the WLAN interworking access server 24, the old SGSN 18 maps the P-TMSI to the IMSI. In this way, the old SGSN provides an identification response that includes both the IMSI and appropriate authentication vectors to identify the mobile wireless terminal 16. If unable to identify the mobile wireless terminal 16, the old SGSN 18 provides an appropriate error message.

5. After establishing the user's identity from the mapping performed by the old SGSN 18, the wireless LAN 14 will verify that the user of the mobile wireless terminal 16 constitutes a valid user and is entitled to use the Wireless LAN.

6. . When a user moves away from the wireless LAN and transitions back to wireless telephony network, the WLAN interworking access server 24 serves as "old" SGSN. Upon request, it sends an identification response to a new SGSN in the wireless telephony network to which the user terminal is being attached.

The identification and verification technique of the present principles affords the advantage of providing secure user identification while minimizing repeated access of the HLR 20 by the WLAN interworking access server 24. Instead of broadcasting a permanent wireless LAN identifier easily intercepted by others, the identification technique of the present principles makes use of the secure identification process of the wireless telephony network 12. Thus, the identity of the user of the mobile wireless terminal 16 remains protected upon a transition from the wireless telephony network 12 to the wireless LAN 14.